

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CHAD W. MERCER and LEE P. NOEHRING

Appeal 2007-2120
Application 09/911,149
Technology Center 2100

Decided: October 24, 2007

Before KENNETH W. HAIRSTON, JEAN R. HOMERE, and JOHN A.
JEFFERY, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1-8 and 36. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

STATEMENT OF THE CASE

Appellants invented a method for establishing secure communications between computers via a network. The invention uses a security standards framework (“IPSec”) that allows a system to select required security protocols, determine the appropriate security algorithm, and implement any required cryptographic keys. To this end, data structures known as security associations (SAs) are utilized which comprise predetermined data fields: (1) the IP destination address; (2) security protocol; and (3) a Security Parameter Index (SPI).¹

The SAs are stored in a Security Association Database (SAD). Conventionally, accessing the SAD involved creating a hash key from the three values constituting the SA to hash into the SAD and thereafter conducting a linear search for a match.²

The claimed invention, however, improves on this approach by assigning the specific memory address value of the stored SA as the SPI value. Such an improvement eliminates the need for elaborate and time consuming SAD table lookup algorithms. The invention also allows fast and efficient SA lookup without significantly impacting memory access bandwidth (Specification 4:5-26, 10:22-26).

Claim 1 is illustrative with the relevant limitations in dispute emphasized:

¹ The SPI is a randomly generated 32-bit value that distinguishes among different SAs established at the same destination address and using the same security protocol (Specification 3:3-6).

² See generally Specification 1:15 - 3:24.

1. A method of establishing a secure communication channel for information flow between two or more computers communicating via an interconnected computer network, comprising:

receiving a security association data structure from one or more computers via the interconnected computer network;

storing the received security association data structure in a memory region having a specific memory address value associated therewith; and

assigning the specific memory address value as a security parameter index value associated with the received security association data structure.

[Emphasis added.]

The Examiner relies on the following prior art references to show unpatentability:

Nessett	US 6,055,236	Apr. 25, 2000
Badamo	US 2002/0184487 A1	Dec. 5, 2002 (filed Mar. 23, 2001)
Carman	US 6,845,449 B1	Jan. 18, 2005 (filed Jul. 21, 2000)

Internet Protocol: DARPA Internet Program Protocol Specification (RFC: 791), DARPA Info. Proc. Tech. Office, Sept. 1981 (“RFC791”).

1. Claims 1, 4, and 36 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Carman.
2. Claims 2, 6, and 8 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Carman and Badamo.
3. Claims 3 and 7 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Carman, Badamo, and RFC791.
4. Claim 5 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Carman and Nessett.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

OPINION

The Anticipation Rejection

We first consider the Examiner's rejection of claims 1, 4, and 36 under 35 U.S.C. § 102(e) as being anticipated by Carman. Anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is capable of performing the recited functional limitations. *RCA Corp. v. Applied Digital Data Systems, Inc.*, 730 F.2d 1440, 1444, 221 USPQ 385, 388 (Fed. Cir. 1984); *W.L. Gore and Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983).

The Examiner has indicated how the claimed invention is deemed to be fully met by the disclosure of Carman (Answer 3-4). Regarding independent claims 1 and 36, Appellants argue that Carman does not disclose *assigning the specific memory address value* as a security parameter index (SPI) value associated with the received SA data structure, as claimed. Appellants note that Carman teaches "using" the SPI to access the security association database (SAD) -- a teaching that merely describes what is generally known in the art (i.e., using the SPI value to create a hash key that

is used to hash into the SAD). Appellants emphasize, however, that this general teaching does not mean that the SPI is the *specific address value* in the SAD at which the associated SA is stored (Br. 5; Reply Br. 2) (emphasis added).

The Examiner contends that the SPI in Carman is the sole value used to access the SAD to store and retrieve the SA. According to the Examiner, since Carman does not teach hashing the SPI or using any other value in connection with the SPI to retrieve the SA from the SAD, the reference therefore teaches assigning the specific memory address value as an SPI (Answer 8-9).

The issue before us, then, is whether Carman's utilization of an SPI to access the SAD reasonably constitutes *assigning the specific memory address value* of the received and stored SA *as an SPI value* as claimed (emphasis added).

We will not sustain the Examiner's rejection of independent claims 1 and 36. Carman discloses an adaptive cryptographically synchronized authentication (ACSA) system that selects an appropriate authentication mechanism ("gear") used to authenticate data exchanged between nodes that share a given SA (Carman, col. 4, ll. 14-28; col. 5, ll. 35-38; Fig. 3). To this end, Carman's ACSA system includes four high-level software modules that implement various security standards: (1) ACSA Controller module 810; (2) IPsec module 820; (3) PF_KEY module 830; and (4) IKE module 840 (Carman, col. 9, ll. 23-34; Fig. 8).

Carman details the authentication process and gear determination using these modules in Figure 9. The relevant steps of this process pertaining to this appeal begin at Step 916. In that step, IKE module 840

sends the SPI and SA information to PF_KEY module 830 for storage in a security policy database (SPD) and SAD respectively (Carman, col. 17, ll. 56-60; Fig. 9).

After Security Association Resource Manager (SARM) 814 sets the appropriate gear that IPsec module 820 should apply when generating an authentication tag, the IPsec module processes outbound IP packets by retrieving the appropriate SPI from the SPD in PF_KEY module 830. The retrieved SPI is then *used* to access the SAD to retrieve the appropriate authentication gear information. Then, IPsec module 820 (1) computes the authentication tag using the selected gear; (2) constructs the authentication header; and (3) forwards the processed IP packet to the next processing function (Carman, col. 17, l. 61 - col. 18, l. 56; Fig. 9 (Steps 918-922) (emphasis added)).

As this passage indicates, Carman teaches storing the SA in the SAD; a database that would certainly include a memory region with a specific memory address value, as claimed. But we fail to see how this specific memory address value is *assigned* as the SPI value itself.

Although Carman indicates generally that the retrieved SPI is “used” to access the SAD to retrieve the appropriate gear information, Carman does not further explain what exactly constitutes this “use” of the SPI. Certainly, the SPI’s index function suggests that it functions, at least in part, as an index or pointer to data contained within the SAD. But Carman does not say whether the SPI is hashed or used with any other value to retrieve the SA from the SAD. Therefore, Carman is, at best, ambiguous on whether the SPI is the “sole value” used to access the SAD as the Examiner asserts.

In any event, even if Carman uses only the SPI as a pointer to the SAD to retrieve associated SAs, the reference stills fall short of *assigning* the *specific memory address value* of the received and stored SA *as an SPI value* as claimed. At best, the SPI value in Carman is *related to or corresponds with* the memory address value of the stored SA in the SAD in some way. But the exact relationship or correspondence is unclear from the reference. The claims, however, require more than mere correspondence. Once received and stored, the SA's specific memory address value is then *assigned* as the SPI value itself. Carman simply does not teach or suggest this feature.

For the foregoing reasons, we will not sustain the Examiner's rejection of independent claim 1 or 36. We will also not sustain the Examiner's rejection of dependent claim 4 for similar reasons.

The Obviousness Rejections

With regard to the rejections under 35 U.S.C. § 103(a) of (1) claims 2, 6, and 8 as unpatentable over Carman and Badamo, (2) claims 3 and 7 as unpatentable over Carman, Badamo, and RFC791, and (3) claim 5 as unpatentable over Carman and Nessett, we find the addition of Badamo, RFC791, and Nessett do not cure the deficiencies of Carman noted above with respect to independent claims 1 and 36. Accordingly, the Examiner's obviousness rejections are also not sustained.

Duplicate Claims

Lastly, we note that claims 2-4 are identical to claims 6-8. Accordingly, the Examiner is reminded that if claims 1-4 are ultimately

Appeal 2007-2120
Application 09/911,149

found allowable, the Examiner must object to claims 6-8 as duplicating the allowed claims. *See* MPEP § 706.03(k).

DECISION

We have not sustained the Examiner's rejections with respect to any claims on appeal. Therefore, the Examiner's decision rejecting claims 1-8 and 36 is reversed.

REVERSED

rwk

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, STE. 325
SCOTTSDALE, AZ 85251